



Naval Criminal Investigative Service



[www.ncis.navy.
mil](http://www.ncis.navy.mil)

Naval Criminal Investigative Service



NCIS is a worldwide federal law enforcement organization whose mission is to prevent terrorism and related hostile acts against DoN forces and installations; protect DoN systems and information against compromise and Reduce criminal activity and mitigate its impact on Navy and Marine Corps operational readiness. NCIS has

civilian special agents and analysts located in over 150 Only





Background

- Due to increased Congressional scrutiny the Department of Defense created a Charge Card Task Force, which issued a report in 2002.
- In accordance with the recommendations of the report, the DoD IG mandated additional requirements. Those pertaining to NCIS regard command notification of GPC abuse case initiation and the immediate revocation of cards.

Background

- Over the past five years NCIS has investigated over 140 cases involving government credit card abuse, which have resulted in a combined loss of over \$400 million dollars.





Investigation

- When possible *criminal* wrongdoing, fraud, or abuse of authority involving a government purchase or travel card is identified, an investigation is initiated.
1. Cardholder's commander and the command security manager must be advised within 72 hours.
 2. Instances that are *substantiated* are reported to DoN Central Adjudication Facility.
 3. The commanding officer must immediately suspend access to classified

Investigation

- Government Credit Card cases fall within the Unauthorized Services Case Category:
- Fraudulently obtained services or unauthorized purchases and fraudulent use of U. S. Government credit cards (not involving forgery) or other charge accounts including telephone calling cards where the victim is the government.



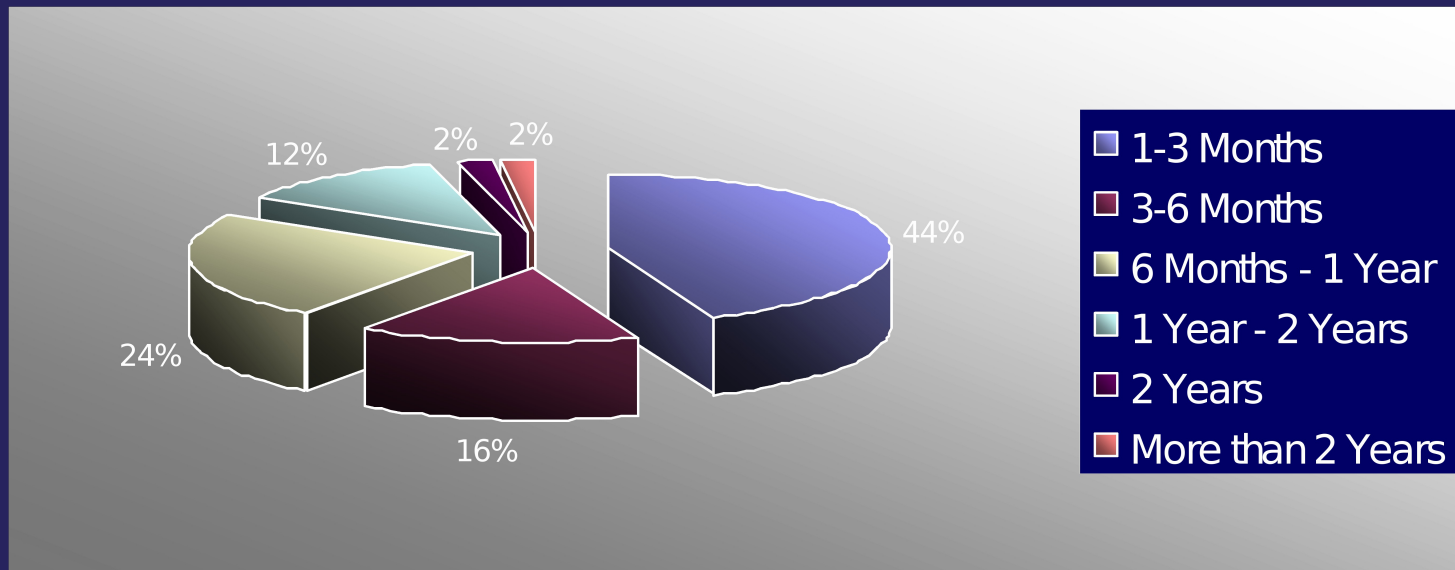


Investigative Steps

- Interviews conducted
- Leads sent to field offices world wide
 - Reporting requirements require a response
- Records reviewed
- Analytical products used to track missing money, perform link analysis and identify patterns of criminal activity
- Interrogations performed when necessary
- Cooperating witnesses identified
- Investigations updated every 60 days

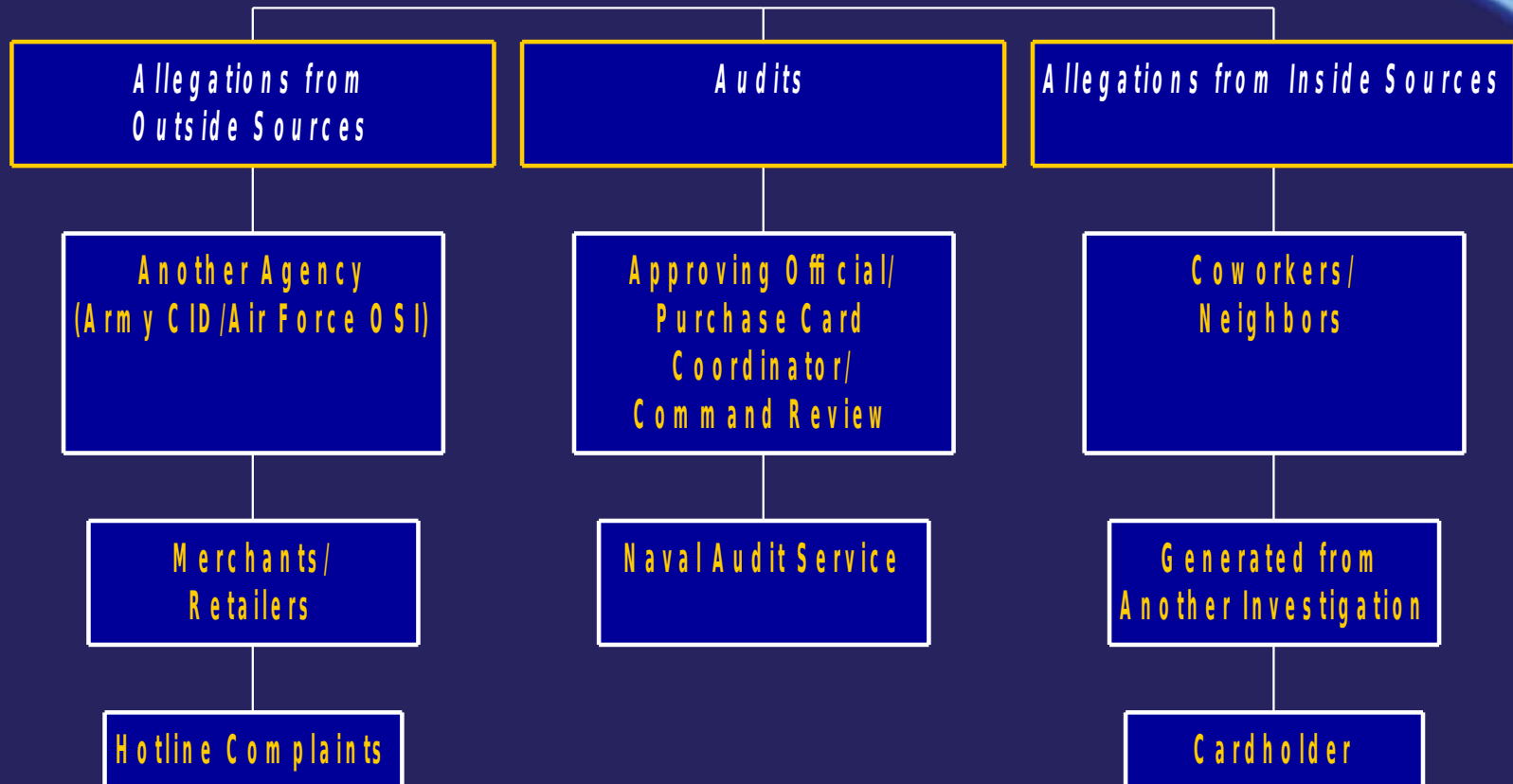
Cases: Duration of Abuse

- The duration of abuse is usually under a year and most often occurs for no more than three months.





Reports of Abuse



Outside Source: Another Agency

- Army CID alerted NCIS that Navy members were involved in procurement fraud utilizing GPC's. An investigation involving the FBI, DCIS, and CID identified two schemes commonly used by DoD personnel.
 1. Vendors provide monetary inducements to DoD employees for their use of GPC's with those vendors.
 2. GPC's are charged for items never delivered. The vendor keeps the profit it would normally receive from the transaction, and the DoD employee pockets the remaining amount of money charged to the government purchase card.





Outside Source: Merchant / Card Company

- Home Depot Security contacted Base Security to report suspicious activity.
 - Stereo equipment purchased with GPC.
- Credit Card company reported that an employee working in their government card service department obtained names, addresses, numbers and account #'s of GPC holders.
 - Used information for ATM cash advances after co-conspirators posed as card holders and requested a new card to replace a damaged card while they were on travel.

Outside Source: Hotline Complaints

- USMC IG and NAVINSGEN (Hotline Div.) are required to submit to NCIS all cases from that are criminal in nature.
- NCIS reviews for investigative merit and possible investigation.
- NCIS may forward to the field for their review and investigative determination.
- All IG commands are required to follow up any NCIS response.





Audits: Command Review

- Approving officials are the first level of oversight. Command financial and credit card managers, therefore:
 1. Provide monthly reports to command security managers identifying accounts with delinquencies exceeding 90 days.
 2. Report any instances of suspected fraud

Audits: Naval Audit Service

- Periodic Audits are performed by both the Naval Audit Service and the DoD IG.
- NCIS can request audits from NAS when circumstances arise where they are needed by sending a formal request from Headquarters in Washington, DC to NAS Headquarters.





Inside Sources: Coworker/ Neighbor

- Individuals from same Unit went to an on base residence to socialize and found a large amount of government property. The appropriate members of command were notified.
- A subsequent Investigation revealed additional abuse and the involvement of other Department of Navy members.

Inside Sources: Generated from Another Investigation

- An investigation of one individual led to the discovery that two others at different locations were falsifying purchase requests and price quotes from vendors to facilitate a theft scheme. They used card number of other's who were unaware of the scheme to make purchases.



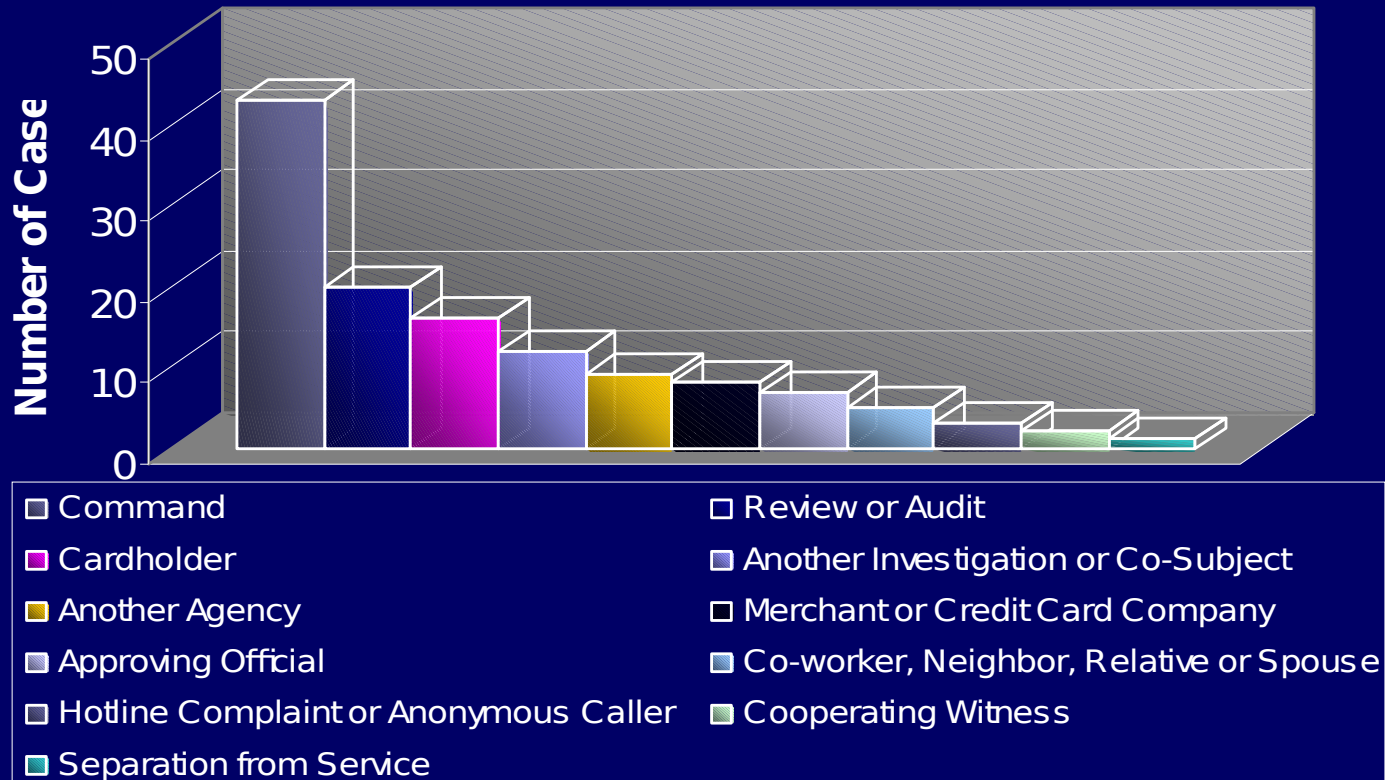


Inside Sources: Cardholder

- Cardholder noticed that credit card Statements reflected payments made to Allstate insurance, Voicestream and a camera company.
- Payments were made online making it difficult to identify subjects.

Detection

The majority of credit card misuse is detected through audits and investigations initiated by the cardholder's command.



Analysis



- Purchase card abuse is often due to lack of oversight.
 - Forging of Signatures
 - No diffusion of duties, card holders often approve own purchases
- Lack of familiarity between Authorizing Officials and Card Users
 - Card user's financial situation (debt)
 - Disgruntled employees

Case Study: lack of oversight

- Subject utilized Government For Purchase Only Authorization Card (FPOAC) to make 84 unauthorized transactions over a 1 year period totaling \$81,122.44.

Import and Domestic Auto Parts	8 Transactions	\$7,826.30
Circuit City	3 Transactions	\$1,247.93
AT &T Wireless	1 Transaction	\$839.55
Safety-Kleen Corporation	22 Transactions	\$45,000.89
Staples	8 Transactions	\$3,825.09
Home Depot	8 Transactions	\$7,005.17
Sprint PCS	7 Transactions	\$2,564.33
Office Max	2 Transactions	\$307.36
Sterling Financial Services	1 Transaction	\$2,163.55
PC Mall and Mac Mall	22 Transactions	\$11,542.78





Case Study: lack of oversight

- Subject was authorized to utilize the FPOAC for vender and contract services but was not authorized to make purchases of any type.
- Lack of detailed oversight, subject kept organized logs that at first glance seemed legitimate.
- Subject has agreed to pay full restitution to the U.S. Navy and plea negotiations are pending.

Analysis

- Increase spot and surprise reviews
- Increase partnerships with commands
- Verify justification for purchases
- Enforce documentation, NAS can't be effective without records
- Verify orders are properly inventoried and accounted for
- Check authorization





Trends

- Increase in GPC's used to pay for medical treatment and physical enhancements.
- Computer crimes are on the rise.
 - Online purchases are more difficult to verify, especially when made overseas.
 - Internet allows companies to hide behind other names that might appear legitimate.

Intra-Agency Sharing

- NCIS forms partnerships with other DCIO's to identify government credit card scams.
- NCIS shares statistics and analysis on closed cases.

